PUBLICAÇÃO

89

ISSN: 0101-9562
ISSN ELETRÔNICO: 2177-7055

SEQÜÊNCIA

Estudos jurídicos e políticos

Publicação do
Programa de Pós-Graduação em Direito da UFSC

VOLUME 42 ▪ ANO 2021

SEQUÊNCIA – ESTUDOS JURÍDICOS E POLÍTICOS é uma publicação temática e de periodicidade quadrimestral, editada pelo Programa de Pós-Graduação Stricto Sensu em Direito da Universidade Federal de Santa Catarina – UFSC.

SEQUÊNCIA – ESTUDOS JURÍDICOS E POLÍTICOS is a thematic publication, printed every four months, edited by the Program in law of the Federal University of Santa Catarina – UFSC.

Versão eletrônica: http://www.periodicos.ufsc.br/index.php/sequencia

A publicação é indexada nas seguintes bases de dados e diretórios/
The Publication is indexed in the following databases and directories:

Base OJS
Base PKP
CCN (Catálogo Coletivo Nacional)
Dialnet
DOAJ (Directory of Open Access Journals)
EBSCOhost
Genamics Journalseek
ICAP (Indexação Compartilhada de Artigos de Periódicos)
Latindex
LivRe!
OJS
PKP
Portal de Periódicos UFSC
Portal do SEER
ProQuest
SciELO
Sherpa/Romeo
Sumarios.org
ULRICH'S
vLex

Ficha catalográfica

Seqüência: Estudos jurídicos e políticos. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. n.1 (janeiro 1980)-. Florianópolis: Fundação José Boiteux. 1980-.

Publicação contínua

Resumo em português e inglês

Versão impressa ISSN 0101-9562

Versão on-line ISSN 2177-7055

1. Ciência jurídica. 2. Teoria política. 3. Filosoia do direito. 4. Periódicos. I. Universidade Federal de Santa Catarina. Programa de Pós-graduação em Direito

CDU 34(05)

Catalogação na fonte por: João Oscar do Espírito Santo CRB 14/849

DOI https://doi.org/10.5007/2177-7055.2021.e71337

A democracia e a tecnologia blockchain

Democracy and blockchain technology

Mateus de Oliveira Fornasier[1]
[1] Universidade Regional do Noroeste
do Estado do Rio Grande do Sul, Ijuí, Brasil

Resumo: Este artigo objetiva estabelecer uma confluência entre o desenvolvimento da tecnologia blockchain e a evolução dos processos democráticos. Resultados: apesar das promessas de transparência e audibilidade que os sistemas de votação eletrônicos parecem oferecer, parcimônia e amadurecimento tecnológico são requisitos necessários para se construir uma democracia eletrônica embasada em tecnologia de cadeias de blocos. Metodologia: método de procedimento hipotético-dedutivo, de abordagem qualitativa e técnica de pesquisa bibliográfico-documental.

Palavras-chave: Blockchain – Democracia Eletrônica – Eleições.

Abstract: This article aims to establish a confluence between the development of blockchain technology and the evolution of democratic processes. Results: despite the promises of transparency and audibility that electronic voting systems seem to offer, parsimony and technological maturity are necessary requirements to build an electronic democracy based on blockchain technology. Methodology: hypothetical-deductive procedure method, with a qualitative approach and a bibliographic-documentary research technique.

Keywords: Blockchain – Electronic Democracy – Elections.

1 INTRODUÇÃO

Nos Estados Unidos da América, o Condado de King, que abriga a cidade de Seattle, foi a primeira região do país a permitir

o voto de todos os eleitores via smartphone. No referido processo, cerca de 1,2 milhão de eleitores puderam participar da votação para o Conselho de Supervisores diretamente de suas residências, utilizando o smartphone, entre 22 de janeiro e 11 de fevereiro de 2020 (Marques, 2020). A expectativa é de que mais eleitores sejam atraídos para participarem do pleito devido à facilidade do processo, transformando e fortalecendo a democracia do país, onde o voto não é obrigatório. Naquele país, a votação feita por aplicativo de celular já existe desde 2018, na Virgínia Ocidental, para permitir que eleitores que vivem no exterior possam indicar seus candidatos. Em Utah, o sistema também é permitido para pessoas com deficiência. Em ambos os casos há o uso de blockchain, o que significa que cada voto é protegido por criptografia – sendo, portanto, um processo mais seguro contra fraudes, a princípio. Contudo, apesar de ser uma das mais importantes democracias do Ocidente, os EUA não ofereceram a experiência pioneira em eleições pela internet: a Estônia é pioneira quanto a isso, com um sistema de votos eletrônicos criado em 2005, que é utilizado por cerca de 30% dos cidadãos. Em tal país, os eleitores possuem um registro digital com um código único que identifica cada indivíduo.

Com essas novidades, pesquisar o uso de tecnologias digitais, como a blockchain, em eleições, é de grande relevância para a sociedade, visto que a queda da confiança nas democracias no Ocidente ultimamente retratadas — que ora têm como causa, ora como consequência, vitórias de candidatos populistas, a presença cada vez maior de radicalismos nos discursos (populares e políticos), retrocessos nos direitos sociais e escândalos de corrupção institucionalizada — demanda a busca por soluções que possam fortalecer a participação do povo em procedimentos de escolha. Já para as ciências sociais em geral, trata-se de um novo modo de pensar a tecnologia em sociedade, não apenas para uma crítica às negatividades que esta possa trazer às interações, organizações e sociedade, mas também para que novas possibilidades benéficas de seu uso possam acarretar melhorias para a

democrática. Por fim, para os estudos jurídicos, tanto o tema das novas tecnologias quanto o da democracia são de fundamental importância para os direitos fundamentais dos cidadãos e para a continuidade de um Estado Democrático de Direito.

O problema desta pesquisa pode ser descrito no seguinte questionamento: que características da tecnologia blockchain podem contribuir para a formação de uma (cripto)democracia? Como hipótese, apresenta-se que a tecnologia blockchain, em razão de suas características básicas — principalmente a desnecessidade de órgãos centrais de controle, o sigilo de sua criptografia e a transparência que ela confere aos processos que a usam como meio — pode ser utilizada para incrementar os procedimentos democráticos ao redor do mundo, de forma que tanto cédulas de votação quanto máquinas eletrônicas para tal possam ser substituídas por sistemas online de votação, que teriam como substrato, além da internet, dispositivos dos próprios eleitores (smartphones, computadores pessoais, etc.), tornando-se desnecessárias as votações *in loco*. Ademais, não apenas as votações periódicas (escolhas de representantes parlamentares, de ocupantes de cargos da Administração Pública, etc.), mas também, a iniciativa popular poderia se fortalecer, fazendo com que uma aproximação maior da democracia direta seja possível.

O objetivo geral dessa pesquisa é estabelecer uma confluência entre o desenvolvimento da tecnologia blockchain e a evolução dos processos democráticos. A fim de concretizar esse objetivo geral, o artigo foi dividido em duas seções, cada qual correspondente a um objetivo específico seu. Nesse passo, o texto se dedica a investigar possibilidades e óbices da tecnologia blockchain para o delineamento de uma cripto-democracia. Assim, são analisadas as confluências entre o desenvolvimento da tecnologia blockchain e a evolução da democracia no século XXI.

Metodologicamente, este é um estudo de natureza exploratória, cujo método de procedimento é o hipotético-dedutivo, com abordagem qualitativa e técnica de pesquisa bibliográfico-documental.

2 POSSIBILIDADES E ÓBICES DA TECNOLOGIA BLOCKCHAIN PARA O DELINEAMENTO DE UMA CRIPTO-DEMOCRACIA

Talvez uma das definições mais sucintas das origens e do funcionamento da blockchain tenha sido sintetizada por Jane Susskind (2017, p. 798-799). Essa forma de tecnologia teria sido projetada por Satoshi Nakamoto em 2008 para permitir que pessoas façam transferências diretas de valor online. Nakamoto teria estabelecido as bases para esse sistema de pagamento eletrônico ponto a ponto, chamado bitcoin. Para o sucesso do seu procedimento, seu criador reconheceu a necessidade de um meio de verificação disponível às partes para que pudessem se certificar de que o dinheiro envolvido em uma transação ainda não havia sido gasto. Portanto, o blockchain fornece um protocolo distribuído que pode ser usado para verificar transações.

Importante acerca da tecnologia é que não é necessário um terceiro confiável (como um banco) para administrar ou verificar transações: ela é totalmente descentralizada, permitindo que qualquer pessoa analise independentemente as transações, conforme um conjunto predeterminado de regras, as quais não podem ser alteradas por ninguém, e são determinadas por uma função matemática denominada "função hash". Trata-se de uma tecnologia segura contra tentativas de adulteração de transações individuais, porque a assinatura criptográfica da transação mais recente é criada usando a assinatura da transação anterior. Portanto, qualquer um que tente modificar uma transação depois que ela tenha sido adicionada ao registro de operações não será bem sucedido porque qualquer pessoa com uma cópia do registro (o blockchain em si) poderá comparar as assinaturas eletrônicas e perceber que a tentativa de adulterar é falaciosa. Assim, criou-se um sistema baseado em provas matemáticas (e não em confiança), eliminando-se a necessidade de uma instituição centralizada para verificar transferências, aumentando assim a integridade financeira e reduzindo os custos de transação.

A criptografia pode ser usada para permitir votação digital segura e anônima nas eleições democráticas — basta substituir a *operação econômica* pela *operação de voto* nos eventuais sistemas eleitorais que venham a integrá-la. Filosoficamente analisando essa possibilidade, tem-se que ela deriva da chamada "instrumentalização secundária", a qual pode ser explicada, conforme exposto por Andrew Feenberg (2018, p. 24, grifos nossos):

> A "instrumentalização secundária" opera ao nível dos significados. Repõe no mundo o elemento da natureza extraído pela instrumentalização primária, integrando-o no mundo social. Simultaneamente orienta o sujeito técnico para os significados sociais criados pela tecnologia. Porque são significados, são apreendidos numa relação hermenêutica que permite diferenças na interpretação, consciência e critica. A instrumentalização secundária *viabiliza intervenções para além do uso previsto para a tecnologia*.

Explicando-se, ao passo que o processo de instrumentalização primária "descontextualiza o fenômeno [natural] para o incorporar num dispositivo" (Feenberg, 2018, p. 24) — ou seja, possibilidades matemáticas criptográficas são convertidas em linguagem de máquina para possibilitar um aparato de registro confiável e auditável de trocas econômicas (de criptomoedas) — na instrumentalização secundária esse aparato técnico é ressignificado e emula uma relação hermenêutica por usuários, analistas e críticos.

Susskind (2017, p. 826-827), da sua parte, aponta para a necessidade de transição radical pelos quais os procedimentos eleitorais devem passar — e exemplifica essa necessidade de modernização utilizando, exatamente, o caso da internet: apesar de enigmática no início da sua popularização, atualmente mais de 3,8 bilhões de usuários em todo o mundo têm na rede um meio essencial para buscar relações pessoais (por aplicativos como o Tinder), transmissão de identidades (mediante plataformas sociais), revelação de esperanças e aspirações (em 140 caracteres ou menos no Twitter), cumprimento de obrigações

tributárias, realização de compras e atividades econômicas, educação (plataformas de EaD), registros (inclusive de alistamento eleitoral), angariação de fundos (mediante crowdsourcing e crowdfunding), realização de campanhas políticas, realização de pesquisas de opinião pública, dentre outras atividades, diretamente relacionadas com a democracia ou não. Mas mesmo com toda essa inserção social, as eleições permaneceram relativamente inalteradas, com a maioria das votações ocorrendo em locais físicos de votação.

A importância da criatividade e modernização no avanço do processo democrático é fundamental. A inclusão da votação em blockchain na definição de sistema de votação pode ser uma inovação, pelos Estados. A inclusão de especialistas em criptografia nos órgãos e instituições governamentais encarregados dos procedimentos de votação, mediante os devidos procedimentos legais e regulamentação legítima seria, assim, um importante passo a ser dado em direção a um sistema mais seguro, atualizado e confiável.

A blockchain tem recebido recentemente uma atenção crescente da indústria, da pesquisa e da mídia, pois permite a criação de um livro compartilhado (mundialmente) mantido em uma base ponto a ponto, onde programas autônomos (os contratos *smart*) podem ser executado. De uma perspectiva tecnológica, ainda é necessário solucionar uma série de questões relacionadas à tecnologia de blockchain para sua adoção convencional, principalmente em relação à escalabilidade e à sua complexidade (que requer habilidades técnicas para uso).

Um pequeno glossário de termos correntes quando se trata dessa forma de tecnologia (obviamente, não extenuante) pode ser descrito abaixo (Gatteschi; Lamberti; Demartini, 2020, p. 93-94):

i) Transações (*transactions*): transferências de criptomoeda de uma parte para outra são representadas como transação de A para B. É útil observar que as criptomoedas não são objetos físicos nem de software, mas sim, o resultado de transações de entrada e saída relacionadas a um endereço;

ii) Blocos (*blocks*): as transações são agrupadas em blocos, que são adicionados periodicamente à blockchain. Cada bloco coleta todas as transações feitas em um determinado período de tempo. Os blocos são ordenados sequencialmente, vinculando cada novo bloco ao anterior;

iii) *Hash*: em criptografia, um hash é um resumo alfanumérico dos dados, calculado a partir da aplicação de uma função matemática a alguns dados de entrada, para produzir uma saída de tamanho fixo;

iv) Nós (*nodes*): ao contrário do que ocorre com bancos de dados centralizados, o blockchain está espalhado por computadores em rede. Esses computadores são chamados de "nós" da rede. A depender do tipo, os nós podem conter uma cópia local da blockchain (criando, assim, cópias redundantes dela) ou partes dela;

v) Consenso da maioria (*majority consensus*): geralmente, a blockchain é mantida por nós da rede, sem uma autoridade central (embora algumas estruturas da blockchain possam prever certo grau de centralização). Para evitar o controle de uma autoridade central, as decisões na rede são tomadas de acordo com um consenso majoritário. Nessa visão, um bloco de informações só será adicionado à blockchain se a maioria dos nós concordar com um novo bloco;

vi) Mineração (*mining*): dependendo do tipo, os nós podem armazenar uma parte ou todo o histórico de transações anteriores ocorridas na blockchain. Também podem decidir se armazenam passivamente uma cópia do blockchain ou se participam ativamente de sua manutenção — em alguns casos, eles recebem uma compensação monetária por essa tarefa. A manutenção da blockchain é o chamado processo de "mineração". Durante o processo de mineração, os nós verificam se uma pessoa tem direito a gastar uma determinada quantidade de criptomoeda e adiciona

novos blocos de informação à cadeia. Dependendo do mecanismo escolhido para adicionar blocos, os nós podem competir uns com os outros para resolver um problema matemático intensivo em computação (projetado para limitar a possibilidade de entidades mal-intencionadas falsificarem transações).

vii) Carteira (*wallet*): as pessoas têm de confiar em carteiras para transferir criptomoedas — pois estas não são objetos, mas sim, resultados eletrônicos de transações anteriores relacionadas a um endereço. Para acionar uma transação, o usuário deve inserir suas credenciais (ou seja, sua chave privada). Uma carteira pode ser usada para armazenar essas credenciais, "assinar" a transação — ou seja, certificar sua imutabilidade e o envio do registro da transação por um determinado endereço — e transmitir a transação na rede blockchain. Cada carteira está associada a um endereço exclusivo (ou mais). Em caso de perda de credenciais, as criptomoedas pertencentes a um usuário não "desapareceriam" da blockchain; em vez disso, o usuário não poderia mais transferi-los para outros endereços;

viii) Contratos inteligentes (*smart contracts*): pequenos programas armazenados no blockchain, que podem se comportar de maneira autônoma se algumas condições forem atendidas. Constituem uma ferramenta poderosa que permite uma variedade de novas aplicações. Uma vez armazenado na blockchain, o código de um contrato inteligente não pode ser alterado, e pode ser inspecionado por todos, mesmo que algumas habilidades de programação ainda sejam necessárias para entendê-lo. Caso algumas situações ocorram, elas podem disparar automaticamente transferências de criptomoeda;

ix) Oráculos (*oracles*): serviços externos, que pegam dados do mundo "real" e os injetam no blockchain (e vice-versa).

Uma possibilidade de aplicação de blockchain bastante discutida, mas que precisaria de considerações adicionais antes da adoção convencional, está relacionado ao gerenciamento de eleições, para o qual garantir a privacidade dos votos seria essencial. Em outras palavras: ao se fazer uma analogia entre *operação de criptomoeda* e *operação de escolha pelo candidato x ou y (ou por proposta a ou b)*, sistemas de votação cuja garantia de sigilo e de registro sem fraudes podem ter nessa tecnologia uma poderosa aplicação, fazendo-se com que a democracia direta/deliberativa seja cada vez mais presente no cotidiano — uma vez que os eleitores poderiam votar em um candidato/proposta a partir de aplicativos em smartphones ou em outros dispositivos similares.

Eleições livres, periódicas e com sufrágio universal constituem um dos mais importantes pilares do bom funcionamento das democracias liberais. Não é simples, porém, conduzi-las de modo a respeitar o Estado Democrático de Direito — e escândalos frequentes em vários níveis provam que o papel exercido pelo poder econômico na política (e, mais especificamente, no financiamento de campanhas eleitorais) representa um problema de difícil solução nos parâmetros atuais. O uso da tecnologia blockchain, contudo, tem sido promissor nesse sentido, conforme Serdült (2019, p. 188), que sugere que o uso de uma moeda criptográfica separada, projetada especificamente para o pagamento dos custos de campanhas políticas e publicidade pode ser introduzido para evitar corrupções econômicas em campanhas eleitorais.

A lógica por detrás dessa introdução é que doações e financiamento de campanhas aumentam o risco de corrupção, e que se deve tentar extrair esses fluxos de dinheiro de um mercado em que as transações são difíceis de rastrear. Com a tecnologia blockchain, as campanhas políticas podem ser rastreadas e financiadas por tokens de criptografia pertencentes aos cidadãos. Esses comprovantes de criptografia podem ter duração e valor nominal, podendo ser emitidos e distribuídos para todas as eleições ou mesmo para uma legislatura completa. Caso seja necessário, vouchers adicionais podem ser liberados. Cada país ou círculo eleitoral poderia, portanto, criar seus próprios

comprovantes dentro de algumas horas. O sistema de blockchain sugerido permitiria rastrear todos os fluxos da moeda criptográfica da campanha e manter o valor total gasto sob controle. No entanto, a inovação discutivelmente mais importante da abordagem sugerida não é apenas o aspecto técnico em si, mas principalmente aquele concernente ao envolvimento direto dos cidadãos. Todo eleitor registrado passaria a ter uma participação pequena, mas direta, na corrida eleitoral. Como um efeito colateral muito bem-vindo, o interesse pela política e, portanto, a participação, também poderia aumentar.

Com uma abordagem transdisciplinar que compreende elementos jurídicos, econômicos, tecnológicos e experimentais, a proposta de criar um token de eleição descentralizado mediante tecnologia blockchain dá às autoridades públicas, aos políticos e à sociedade em geral uma inovação nos modos pelos quais o financiamento de campanhas podem ocorrer futuramente. A proposta permite também aos legisladores se atualizarem sobre os desafios futuros relacionados à aplicação da tecnologia blockchain em sistemas políticos democráticos.

É claro que várias questões surgem quando uma proposta dessa magnitude surge. E as seguintes perguntas de pesquisa podem servir como um guia preliminar para o desenvolvimento de futuros estudos de viabilidade. Essas questões poderiam ser agrupadas em quatro domínios (Serdült, 2019, p. 189):

1) *Governança e jurídico:* quais requisitos legais se aplicam a uma criptomoeda para campanhas políticas? Que restrições são impostas pelo princípio da liberdade econômica e quais requisitos devem ser atendidos no que diz respeito à garantia da liberdade eleitoral? Que disposições legais seriam necessárias para a introdução de uma criptomoeda separada para campanhas políticas?
2) *Tecnológico:* Como os tokens devem ser projetados? Como as doações para campanhas mediante o uso de tokens podem permanecer anônimas, mas tornar-se públicas ao atingir um

determinado limite? Podem ser previstos aplicativos seguros e fáceis de usar para uso individual?

3) *Econômico:* Quanto custaria a introdução e administração de tokens de campanha em relação à administração e ao consumo de energia? Como esses custos podem ser financiados?
4) *Comportamental:* Como os cidadãos reagem à ideia de criar tokens para financiar campanhas políticas? Eles estariam dispostos a usá-los? Quais padrões de uso de token podemos observar?

O blockchain tem potencial para democratizar ainda mais um grande número de estruturas — tornando muito mais eficientes as estruturas estabelecidas e promovendo a autodeterminação dos cidadãos, o que pode vir a neutralizar o desencantamento popular com a política. Contudo, há ainda sérios óbices à implantação mais difundida dessa forma tecnológica nas instituições, devido principalmente ao fato de que muitos políticos ainda hesitam em apoiar o Blockchain pelos seguintes motivos (Braun, 2020, p. 239-251): *i) Descentralização dos sistemas:* o blockchain muda as estruturas de poder de uma hierarquia centralizada para estruturas descentralizadas e planas, o que não é necessariamente do interesse dos representantes eleitos, que não têm vontade de renunciar ao poder; *ii) Complexidade técnica:* a complexidade técnica do blockchain dificulta sua compreensão para a maioria das pessoas, inclusive políticos, que, carecendo de um entendimento suficiente da tecnologia, não têm competência para fazerem uma avaliação qualificada de seu potencial benéfico de aplicação e de seus riscos.[1]

[1] Giralda et al. (2019, p. 353) também reforçam a tese do alto grau de desconfiança com que a implementação desse tipo de sistema é percebida por seus eventuais usuários, eis que a grande maioria das pessoas não possui conhecimento específico na área, motivo pelo qual são obrigadas a confiar na palavra de uma empresa ou de um grupo de técnicos treinados para garantir que o sistema funcione corretamente. E até grandes empresas como Microsoft ou Apple precisam emitir atualizações para corrigir bugs em seus códigos. Ademais, inconvenientes também surgem de adversários maliciosos com o objetivo de corromper o seu bom funcionamento. O maior problema da votação eletrônica está nos riscos à segurança: ataques on-line, compra de votos e outras manipulações realizadas por terceiros.

A tecnologia blockchain poderia ser tida como uma ferramenta para conferir ainda mais confiança aos sistemas de votação e eleição democráticos, e aumentar a participação dos cidadãos nos procedimentos democráticos. A proposta de Peter Racsko (2019, p. 15) relacionada a essa tecnologia diz respeito ao uso de protocolos de consenso, que são partes inseparáveis de um sistema útil e prático de blockchain. Os protocolos atualmente existentes são inadequados para uso direto em um sistema de votação. Com todos os protocolos conhecidos, os participantes que desejam desempenhar um papel ativo na verificação da exatidão das transações econômicas precisam sacrificar recursos (tempo ou dinheiro computados), ou precisam ter um certo nível de recursos materiais ou capacidades abertas para realizar uma transação. Além de terem direito de conferirem os processos de verificação das operações, eles também são recompensados com as criptomoedas adquiridas. Na votação democrática, no entanto, todos os eleitores devem ter os mesmos direitos em todos os aspectos, sendo que sua diferença baseada em suas atividades não é uma opção.

A decisão pelo uso de blockchain em eleições democráticas exige a criação de um novo protocolo de consentimento que crie direitos iguais para todos. A verificação, no entanto, deve ser recompensada, porque o sistema não funcionará sem essa motivação. Atualmente, todos os protocolos que satisfazem a condição de direitos e motivações iguais podem ser operados apenas de fora do sistema e, é claro, os protocolos de consenso e seu gerenciamento devem ser transparentes. A tecnologia blockchain sem um protocolo de consenso, como um banco de dados preservado de integração distribuído, naturalmente pode ser usada em um sistema de votação eletrônica, se uma organização externa, por exemplo, um centro de certificação do governo, valida as transações.

O blockchain como banco de dados e centro de certificação pode compreender um modelo de votação online se os eleitores confiarem em uma organização, a qual não podem auditar ou controlar diretamente. A auditoria do blockchain, nessa proposta, seria possível

apenas por uma organização central. A votação online nessa estrutura talvez seja mais eficiente e econômica do que a votação em cédulas físicas, mas o papel do controle central é inevitável e, no nível do sistema, não exclui a manipulação. Para milhões de usuários e investidores de Bitcoin ou outras outras criptomoedas, no entanto, a falta de uma organização controladora central (por exemplo, um banco) é realmente a propriedade mais atraente do sistema.

Para Racsko (2019, p. 15), nenhum dos algoritmos de consenso frequentemente usados no comércio de criptomoedas atende totalmente aos requisitos de segurança um sistema de votação online. O consenso sobre a correção da blockchain e a anonimidade dos eleitores são apenas necessárias, mas não são condições suficientes para uma votação na vida real. A tecnologia blockchain tem um potencial real no desenvolvimento de um sistema de votação seguro, confiável e barato, mas há muitas questões teóricas e práticas que precisam ser tratadas antes que a tecnologia seja aceita, mesmo que seja para testes.

Denny, Ferreira e Castro (2017, p. 138-139) elogiam a tecnologia de blockchain em razão da maior transparência que pode conferir aos mais variados processos, da rastreabilidade de pedidos e decisões por governos, da auditabilidade, da maior velocidade e eficiência (decorrentes, principalmente, das possibilidades de automação dos processos governamentais), da diminuição de danos em razão de falhas humanas e da redução de custos relacionados ao arquivamento de documentos que proporciona. Contudo, apontam que o blockchain talvez ainda seja superestimado, mesmo que muitas vezes seja pouco compreendido. Sua aplicação ainda é restrita, incipiente e problemática no que tange à escalabilidade, à privacidade e à confidencialidade — mas esses deméritos tendem a diminuir com o avanço das tecnologias. Esses problemas exigem cooperação de especialistas, focados em tecnologia, e com expertise em regulação, a fim de que a infraestrutura que atenda a necessidades práticas de implementação de políticas relacionadas a essa tecnologia possa ser estabelecida. São, inclusive, escassas as análises empíricas, sistemáticas e críticas para

traçar os aspectos positivos e negativos, compreender os modelos de negócios e os casos em que já tem havido uso de tal tecnologia, que possam sinalizar arquiteturas de rede recomendáveis e, em razão disso, para se estabelecer sua governança. Esses riscos e incertezas, inclusive relacionados à regulação ou a eventuais efeitos jurídicos decorrentes da má aplicação da ferramenta, fazem com que a implementação seja fragmentada, disputada e complexa.

Sendo uma tecnologia ainda jovem, a blockchain oferece flexibilidade interpretativa. Contudo, à medida que as propostas envolvendo-a se tornam instituições, a interpretação fica sob a influência de forças estruturais, que possuem poderes que se inclinam em algumas direções e não em outras. As estruturas da tecnologia blockchain, segundo Manski e Manski (2018, p. 129), tendem ao desenvolvimento de soberanias mais distribuídas, democratizadas e dotadas de alta tecnologia. Muitas dessas mesmas tendências, todavia, podem ser canalizadas e reformuladas por atores bem preparados e altamente incentivados a tirar vantagem — em outras palavras, empresas e Estados. As empresas, particularmente, têm uma vantagem temporal por serem pioneiras na intimidade para com tais tecnologias, além dos recursos para contratar tecnólogos e influenciar agentes/funcionários do Estado, num esforço de regular o mundo da blockchain no futuro próximo. E contra tais vantagens há pouca probabilidade de resistência desagregada efetiva por parte dos proponentes libertários da soberania individual.

A soberania popular, por outro lado, pode ter um futuro. Movimentos sociais ativistas da democracia podem se tornar capazes de superar suas desvantagens estruturais iniciais, construindo uma coalizão de tecnologias e públicos mais amplos. Grande parte da ideologia motivadora e da prática diária dos codificadores de blockchain é idealista, utópica, descentralista e cooperativa. Ademais, muitos desenvolvedores de blockchain enriqueceram com investimentos iniciais em criptomoedas. Como conconstituintes próximos do novo mundo blockchain, tais desenvolvedores estão em uma posição potencialmente

determinante, sendo suas afinidades importantes. Some-se a isso o forte desejo pelo tipo de sociedade mundial que as cooperativas estão programando em seus aplicativos blockchain que foram articulados na onda da democracia global de 2008-2014, e um aumento da soberania popular global pode não ser tão improvável.

Segundo Marcella Atzori (2015, p. 31-32), há fortes motivos para se desconfiar da aplicação da tecnologia blockchain a serviços públicos em geral — o que pode também ser pensado para procedimentos de tomada de decisão. Embora tenham sido originalmente concebidos como ferramentas de desintermediação, os sistemas de blockchain totalmente distribuídos são caracterizados pela presença de uma grande quantidade de terceiros e empresas lucrativas que oferecem serviços de intermediação, com fortes assimetrias de informações e poder entre desenvolvedores e usuários. Assim, há vários fatores que desafiam a natureza igualitária das redes de blockchain atuais: tendência para a centralização, divisão digital, falta de transparência no processo de tomada de decisão e poder inexplicável dos desenvolvedores principais. E isso faz com que as expectativas de alguns defensores da blockchain sejam superestimadas e irrealistas. Em particular, a ideia de uma autoridade baseada em blockchain "flutuando livremente" acaba sendo enganosa, pois é comprovado que a autoridade se transforma em formas centralizadas mais sutis ou ocultas.

Portanto, existem razões para questionar o papel da governança baseada em blockchain como um grande facilitador do poder individual, em um sentido absoluto. Se por um lado é provável que a promessa de capacitar indivíduos não seja cumprida — em razão do papel dominante dos mercados e dos sistemas de verificação especulativa de cadeias de blocos totalmente distribuídas —, por outro, o processo de subestimar as instituições públicas, o primado da economia sobre a política e a transformação dos cidadãos em clientes com a promessa de mais liberdade, eficiência e igualdade, podem ocultar mais um processo insidioso de corporativização da política, que capacita os mercados em detrimento dos cidadãos. Longe de ser nova, essa mudança de poder

do setor público para o setor privado está ocorrendo de várias formas há décadas, com enormes custos sociais e econômicos.

Um dos grandes problemas técnicos que ainda persiste em relação ao uso massivo da tecnologia de blockchain, conforme apontado por Srivastava, Dwivei e Singh (2018), diz respeito ao tamanho das cadeias de blocos produzidas nas operações e o grande uso de eletricidade — problemas que, somados com a possibilidade de velocidades computacionais muito baixas em alguns casos, podem fazer com que a aplicação massiva desses sistemas de votação em países com grandes disparidades em relação ao acesso à tecnologia pelos eleitores possa ser inviável demais. Além dessas considerações, as estratégias de contagem de votos também desempenham um papel importante em qualquer processo de eleição. Os teóricos dos jogos sugeriram várias tipos de esquemas de votação, cada um com seus benefícios e desvantagens. Os esquemas de contagem de votos que são amplamente utilizados atualmente são:

i) Votação de pluralidade: onde cada eleitor pode votar em apenas um candidato e quem obtiver mais votos é eleito.
ii) Votação classificada: em vez de selecionar apenas um candidato, os eleitores classificam todos os candidatos de acordo com suas preferências, do mais preferido ao menos. Cada país tem um ambiente político e local diferente.

Recentemente acendeu-se, no Brasil, um debate a respeito do voto impresso. Seus defensores argumentam que tal procedimento garantiria a lisura do processo em caso de fraudes eleitorais via *software*: em caso de suspeita de fraudes (ou em falhas dos sistemas de informática) seria possível, assim, realizar a recontagem por meio dos votos impressos. Os críticos dessa proposta, no entanto, tendem a apontar o retrocesso que provocaria, principalmente quanto à economia de recursos, pois a impressão de mais de 140 milhões de cédulas e comprovantes eleitorais iria impactar nos gastos públicos e no meio ambiente. A fim de apresentar mecanismos garantes da lisura dos

procedimentos eleitorais democráticos, mas que garantam economia de recursos, Silva (2018, p. 71 e ss.) propõe o uso de tecnologia blockchain no sistema eletrônico brasileiro de votação. A viabilidade de tal proceder se revela quando consideradas suas principais características técnicas, que trazem vantagens para o processo eleitoral.

Em sua proposta, contudo, não deixa de sopesar que novos procedimentos tecnológicos não podem desconsiderar direitos fundamentais dos cidadãos, a saber, no que tange à matéria em específico, o direito ao sigilo do voto (art. 14, CF/88) e o direito à Administração Pública eficiente (art. 37, CF/88). Como são intrínsecas a essa forma tecnológica as características da transparência nas operações realizadas, da descentralização e da imutabilidade dos dados, além de se garantir lisura de procedimentos e economia de recursos, o caráter secreto do voto e eficiente da Administração seriam respeitados.

É claro que, em se tratando de uma tecnologia bastante recente, uma abordagem transdisciplinar e muita experimentação devem ser conduzidas — visto que se trata de uma mudança de política pública de grande magnitude e importância. Todavia, críticas que partem da premissa da necessidade de reeducação dos eleitores não devem prosperar, visto que, no atual momento da história, cidadãos já acostumados com TICs no cotidiano (para acessar serviços bancários online, redes sociais, portais eletrônicos, etc.) estariam já devidamente capacitados para compreender uma mudança hipotética no sistema eletrônico, com a utilização de digitação de senhas, por exemplo.[2] Ademais, se vier a

[2] Pawade et al (2020), por exemplo, já desenvolveram uma técnica de votação on-line com autenticação biométrica e tecnologia blockchain que se vale do sistema de reconhecimento de íris, que garante que apenas uma pessoa verificada possa votar. Esse sistema não armazena a imagem da íris capturada no banco de dados, extraindo os recursos da imagem da íris e removendo sua imagem da memória, tornando os dados biométricos mais seguros. Esses recursos extraídos (juntamente com todas as outras informações do usuário e os votos expressos por eles) são armazenados no blockchain, o que faz com que o sistema seja transparente, descentralizado e oferecendo fácil detecção a acidentes (tais como adulteração de informações ou alternância de votos). Esse sistema (o qual ainda precisa ser amadurecido) tem precisão média de 81,11% (consequentemente, taxa média

ocorrer, obviamente essa mudança será precedida de amplo esclarecimento junto à população, do mesmo modo que ocorreu quando da mudança do sistema eleitoral do registro físico para a urna eletrônica, por exemplo. Acrescente-se a isso que críticas que apregoam que o uso da blockchain deveria se restringir apenas a criptomoedas olvidam que empresas como a Sony já a utilizam para o controle de direitos digitais. E, também, que países como a Estônia já se valem de sistemas eleitorais online desde 2005, o *iVoting* — sistema este que permite aos eleitores expressarem seu voto a partir de qualquer computador conectado à internet em qualquer lugar do mundo. E, em maio de 2018 ocorreram nos Estados Unidos as primeiras eleições registradas em blockchain naquele país.

Atualmente, todos os usuários da internet (seres humanos e dispositivos) estão conectados a servidores centralizados, que agem como autoridades confiáveis por todos os usuários, possibilitando a troca de informações críticas e dinheiro entre usuários não confiáveis. Mas a manutenção de grandes servidores é dispendioso e não é acessível se esses sistemas digitais para infraestruturas críticas das cidades forem invadidos. A tecnologia blockchain teria o potencial para resolver esses problemas, na opinião de Qi et al. (2017), por ser uma ferramenta que registra todas as transações e eventos digitais que acontecem no mundo virtual. Todos os registros estão abertos a todos os usuários e as assimetrias de informações entre dois usuários são minimizadas — o que impossibilitaria que usuários realizem qualquer forma de trapaça, mesmo sem uma autoridade centralizada.

A votação é um dos fundamentos da democracia, mas o sistema de votação atual tem sido atormentado por fraudes na votação em várias partes do mundo — sendo possível, por exemplo, o registro de vários votos por apenas um usuário (o que pode ser usado por

de falhas de 18,89%). Esses valores se devem ao fato de que a captação da imagem da íris deve se dar com o mínimo de interferência (ruído) de imagem, e não a problemas com a criptografia da blockchain.

qualquer grupo de interesse especial que procure obter vantagem para os candidatos que eles apoiam). Também não há como os eleitores garantirem que seus votos serão registrados e contados com precisão. Assim, mais importante do que *quem vota* é *quem conta os votos* para decidir o vencedor. A fraude na votação frustra as pessoas de acreditarem que seus votos são importantes, então muitas escolhem não votar (obviamente, em democracias onde o voto não é obrigatório). Muitos governos, por isso, se interessaram pela máquina de votar eletrônica para aumentar a transparência da votação, evitando fraudes. Mas mesmo esse sistemas poderiam sofrer com a ação de hackers com eventual acesso físico à máquina de votação ou ao seu cartão de memória removível, instalando um código malicioso capaz de roubar votos sem ser detectado. Ademais, a máquina de votação é geralmente projetada, produzida e mantida por uma única empresa — e é muito difícil provar que tal empresa não instalou códigos maliciosos na máquina desde o início.

Uma votação alimentada por blockchain poderia ser executada da seguinte forma (QUI et al., 2017, p. 518):

i) Antes de votar, um usuário envia sua identificação legal e nome de usuário na blockchain para um verificador de identidade. Após ser aprovado, o usuário receberá sua cédula única. O verificador não é necessariamente o governo, sendo que essa tarefa poderia ser realizada por mineradores de blockchain, que têm o incentivo para se comportar corretamente. Usando a criptografia homomórfica, o processo de verificação pode ser executado diretamente em dados criptografados, sem vazar a identidade do usuário;
ii) Durante a eleição, o usuário completa sua cédula e a envia para as urnas baseadas em blockchain. Cada usuário usa um dispositivo diferente como ponto de entrada para votar, de modo que a invasão maliciosa de um único dispositivo tem pouco efeito nos resultados da votação;

iii) Após a eleição, cada usuário pode auditar os resultados da votação porque pode acessar os dados abertos no blockchain. Além disso, a decisão de um usuário não será conhecida por outros eleitores, pois os usuários usam seu pseudo nome no blockchain ao votar.

Conforme posiciona-se Berg (2017), a democracia representativa é constituída por uma cadeia de delegação de eleitores e uma correspondente cadeia de prestação de contas, com algumas questões (particularmente constitucionais) reservadas ao voto popular. Essa estrutura reflete os altos custos de transação da coordenação de preferências entre uma população grande e diversificada, que em parte foi determinada por limitações tecnológicas. A tecnologia blockchain reduz significativamente os custos de transação, tendo, ademais, implicações significativas para a governança democrática. Em uma cripto-democracia, os eleitores têm relações contratuais que lhes permitem desmembrar, delegar, reorganizar e reservar seu poder de voto.

Uma cripto-democracia seria, então, uma implementação literal de um contrato social, em que cada cidadão tem uma relação contratual para com todos os outros cidadãos, sujeitos a constantes negociações. Numa democracia representativa em padrões atuais, uma eleição representa um comércio contratual a cada três a quatro anos, enquanto uma cripto-democracia permite que centenas de milhares dessas transações ocorram, se não milhões, sujeitas às limitações do software de blockchain.

Numa cripto-democracia, muitas das características centrais da democracia estão ausentes. Na sua forma mais pura, não há eleições. A relação entre representantes e seus eleitores é contratual descentralizada, dissolúvel de acordo com as condições impostas por esse contrato. Tampouco existe necessariamente um parlamento ou um chefe de governo, embora essas estruturas (e outras estruturas ainda não vistas) possam surgir. Em uma cripto-democracia, em vez de planejar ou estruturar instituições políticas, nós as desenvolvemos.

3 CONCLUSÃO

Após toda a argumentação acima realizada, pode-se chegar a algumas conclusões interessantes acerca do uso da tecnologia blockchain na governança. Tem-se, primeiramente, que este apresenta grande potencial de ser direcionado, em sua regulação, conforme os interesses de Estados e, principalmente, de empresas — as quais têm a vantagem do pioneirismo e o capital para investir não apenas em aparatos técnicos, mas também, para influenciar Estados. Contudo, não se pode ser totalmente pessimista, pois revoluções tecnológicas, muitas vezes, começam com indivíduos ou pequenos grupos imbuídos de ideais, que adquirem muitos recursos em razão do seu sucesso, o que faz com que adquiram bastante independência. Ademais, movimentos sociais também podem correr atrás de tais vantagens, tornando o ideal de soberania popular e democratização uma realidade mais afeita aos seus interesses.

Mas o atual estágio do desenvolvimento e uso da tecnologia blockchain para operações econômicas demonstra que as promessas apresentadas quando do seu advento — principalmente no que tange à desintermediação, igualdade entre usuários e individualização — ainda não foram concretizadas. E isso pode ser perigoso para a aplicação de tal forma tecnológica a procedimentos democráticos de decisão (pelo menos enquanto ainda não forem resolvidos os problemas que podem levar a uma nova forma de corporativização da política).

Em segundo lugar, características básicas da tecnologia blockchain — tais como a sua descentralização e a complexidade técnica que acarreta — podem trazer grandes desconfianças quanto à sua aplicação em políticas públicas. Essas características podem ter a antipatia de representantes eleitos que, além de não terem a expertise necessária para compreendê-la, veriam nela um fator de erosão do seu poder dependente de estruturas hierárquicas centralizadas. As possibilidades de maior transparência e audibilidade, mais eficiência, menos erros decorrentes de falhas humanas e de redução de custos relacionados às

necessidades físicas dos processos governamentais também são grandes promessas da tecnologia blockchain à democracia.

Por fim, deve-se analisar que o simples uso de tecnologia blockchain (em qualquer das suas formas) não é o suficiente para uma transformação total da democracia: do ponto de vista técnico, pode-se ter em tal tecnologia, quando somada a outras (tais como biometria), maior transparência a processos de votação, bem como maior atratividade a eleitores de países onde o voto não é obrigatório. Contudo, para além de uma ampla gama de procedimentos e instituições importantes, a democracia é um processo em permanente construção — e o uso de novas tecnologias, por maior que seja a sua importância, deve ser sempre analisada como secundária em relação àquela que talvez seja a principal virtude democrática: o empoderamento do cidadão para tomar decisões que estejam de acordo com o melhor entendimento do que seja o bem público.

Por tais razões, é possível apontar a confirmação parcial da hipótese inicialmente apresentada — de que a tecnologia blockchain, em razão de suas características básicas (desnecessidade de órgãos centrais de controle, sigilo criptográfico e transparência, principalmente), tem grande potencial de ser utilizada para incrementar os procedimentos democráticos, substituindo meios físicos e eletrônicos localizados por sistemas online de votação. Esse fortalecimento pode se dar em não apenas em relação a eleições periódicas para cargos da democracia representativa, mas também em relação à iniciativa popular e a outros procedimentos de democracia direta. Mas tratando-se de uma tecnologia de desenvolvimento ainda incipiente, há vários riscos atinentes ao seu uso difundido demais, sendo aconselhável não apenas o comedimento e a precaução do seu uso em procedimentos democráticos importantes, mas também, sua combinação para com órgãos estatais que possam vir a conferir ainda mais confiança à tecnologia.

Nesse sentido, é importante concluir apresentando novos caminhos para os quais a pesquisa que relacione tecnologias de criptografia (dentre elas, a blockchain) aos processos decisórios democráticos.

Uma via interessante seria realizar uma análise global das influências externas, para além das tecnologias utilizadas para assegurar os resultados dos votos, pois pressões de grupos detentores de poder nem sempre democráticos — tais como forças coatoras (milícias, máfias, etc.) — crises econômicas e conflitos sociais podem forçar os eleitores a opinarem de forma não desejada, escrutinadores a apresentarem resultados diversos, etc. Outra via bastante interessante seria realizar estudos de casos mais pontuais acerca de situações mais concretas de uso da blockchain no contexto democrático.

REFERÊNCIAS

ATZORI, Marcella. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? **Retrieved September**, v. 1, p. 1-37, 2015.

BERG, Chris. Delegation and Unbundling in a Crypto-Democracy. **SSRN**, 2017. DOI: http://dx.doi.org/10.2139/ssrn.3001585

BRAUN, Alexander. Blockchain—The Savior of Democracy? In: FELDNER, Denise (ed.). **Redesigning Organizations:** Concepts for the Connected Society. Cham: Springer, 2020, p. 239-251.

DENNY, Danielle Mendes Thame; FERREIRA, Roberto; CASTRO, Paulo Douglas de. Blockchain e Agenda 2030. **Revista Brasileira de Políticas Públicas, v. 7, n. 3,** p. 122-142, 2017. DOI: http://dx.doi.org/10.5102/rbpp.v7i3.4938.

FEENBERG, Andrew. **Tecnologia, Modernidade e Democracia**. Trad. Eduardo Beira. Lisboa: Inovatec Portugal, 2018.

GATTESCHI, Valentina; LAMBERTI, Fabrizio; DEMARTINI, Claudio. Blockchain Technology Use Cases In: KIM, Shiho; DEKA, Ganesh Chandra (eds.). **Advanced Applications of Blockchain Technology.** Singapore: Springer, 2020, p. 91-114.

GIRALDA, Yamil; VILCHES, Gonzalo Leonel; BRITOS, José Daniel; DÁVILA, Laura Cecilia Díaz. Avances hacia un prototipo de sistema de votación electrónico con base de datos distribuida – Tecnología *BlockChain* In: RIVOIR, Ana; MORALES, María Julia (Org.). **Tecnologías digitales:**

miradas críticas de la apropiación en América Latina 1 ed. Buenos Aires; Montevideo: CLACSO; RIAT, 2019, p. 337-354.

MANSKI, Sarah; MANSKI, Ben. No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World. **Law Critique**, v. 29, p. 151–162, 2018. DOI: https://doi.org/10.1007/s10978-018-9225-z.

MARQUES, Ana. Voto pelo celular: EUA testam a tecnologia em eleições de Seattle. **Seleções Reader's Digest**, 24 jan 2020. Disponível em: https://www.selecoes.com.br/colunistas/voto-pelo-celular-eua-testam-a-tecnologia-em-eleicoes-de-seattle/. Acesso em: 26 mar 2021..

PAWADE, Dipti; SAKHAPARA, Avani; BADGUJAR, Aishwarya; ADEPU, Divya; ANDRADE, Melvita. Secure Online Voting System Using Biometric and Blockchain In: SHARMA, Neha; CHAKRABARTI, Amlan; BALAS, Valentina Emilia (eds.). **Data Management, Analytics and Innovation:** Proceedings of ICDMAI 2019, Volume 1. Singapore: Springer, 2020, p. 93-110.

QI, Renming; FENG, Chen; LIU, Zheng; MRAD, Nezih Mrad. Blockchain-Powered Internet of Things, E-Governance and E-Democracy In: Vinod Kumar T. (eds.). **E-Democracy for Smart Cities:** Advances in 21st Century Human Settlements. Cingapura: Springer, 2017, p. 509-520. DOI: https://doi.org/10.1007/978-981-10-4035-1_17.

RACSKO, Peter. Blockchain and democracy. **Society and Economy,** v. 41, p. 1-17, 2019. DOI: 10.1556/204.2019.007.

SERDÜLT, Uwe. Reconnecting Citizens to Politics via Blockchain: Starting the Debate In: VIRKAR, Shefali et al. (eds.). **Proceedings of Ongoing Research, Practitioners, Posters, Workshops, and Projects of the International Conference EGOV- CeDEM-ePart 2019, San Benedetto Del Tronto, Italy, 2 September 2019 - 4 September 2019**, p. 185-190. DOI: doi.org/10.5167/uzh-175213.

SILVA, Matheus Passos. A segurança da democracia e a blockchain. **Estudos Eleitorais**, Brasília, v. 13, n. 3, p. 71-105, set./dez. 2018. Disponível em: http://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/5961. Acesso em: 26 mar 2021..

SRIVASTAVA, Gautam; DWIVEDI, Ashutosh Dhar; SINGH, Rajani. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology In: **Proceedings of the 15th International Joint Conference**

on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT, p. 508-513, 2018. DOI: 10.5220/0006881905080513.

SUSSKIND, Jane. Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System. **San Diego Law Review**, v. 54, n. 4, p. 785-828, 2017. Disponível em: https://digital.sandiego.edu/sdlr/vol54/iss4/4. Acesso em: 26 mar 2021.

MATEUS DE OLIVEIRA FORNASIER

Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI). Doutor em Direito pela Unviersidade do Vale do Rio dos Sinos (UNISINOS), com Pós-Doutorado pela University of Westminster (Reino Unido).

Endereço profissional: Universidade Regional do Noroeste do Estado do Rio Grande do Sul, R. do Comércio, 3000 - Universitário, Ijuí - RS, 98700-000, Brasil.

ORCID ID: http://orcid.org/0000-0002-1617-4270

E-MAIL: mateus.fornasier@unijui.edu.br

Recebido: 04/02/2020

Aceito: 24/03/2021